

III. CLAIM AMENDMENTS

1. (Currently Amended) A method for establishing and managing a trust model between an identification module and a radio terminal, said method comprising~~characterized in that it comprises:~~

~~authenticating a radio terminal authentication step by said identification module, said identification step authenticating authentication being carried out by means of identification radio terminal authentication means that are provided either to said identification module by a mobile radio-telephony network at the time of an initialization step or similar or at the time of an a so-called updating step, or to said radio terminal by the identification module; and~~

~~a control step controlling by said identification module of at least one specific characteristic of the radio terminal, said specific characteristic being previously transmitted by radio-telephony to said identification module from a secured server of said mobile radio-telephony network.~~

2. (Currently Amended) The method according to claim 1, wherein ~~the lifetime of said radio terminal authentication means present in the identification module are provided with a validity period that is limited by a determined expiration date, said authentication means being comprised of at least one authentication key.~~
3. (Currently Amended) The method according to claim 1, wherein said identification module comprises at least one of ~~is~~ an SIM type chip card, ~~or an USIM card for third-generation networks,~~ or an equivalent card comprising in a memory the representative subscription data.
4. (Original) The method according to claim 1, wherein the identification module maintains a trust relationship with the radio terminal by generating authentication means and then by providing these authentication means to the radio terminal by

secured exchange mechanisms based on authentication means initially available from the radio terminal.

5. (Currently Amended) The method according to claim 1, comprising at the time of said initialization or updating ~~generating-step-a-generation-step~~, carried out at least by said identification module, ~~of a so-called-trust key~~, said trust key being used by said module for encrypting at least data exchanged between the identification module and the radio terminal.
6. (Currently Amended) The method according to claim 2, wherein said initialization step of said authentication means is done on the initiative of the radio-telephony network, after denial of the key initiated by at least one of said module, ~~or the mobile radio-telephony network~~, or the radio terminal, following an expiration of the validity period of the key ~~or even at the time of initialization of the identification module~~.
7. (Currently Amended) The method according to claim 1, wherein said authentication ~~authenticatingstep~~ comprises ~~especially the following steps~~:
 - ~~an-utilization step~~ in the radio terminal of at least one first authentication key memorized in the radio terminal by at least on first authentication algorithm memorized in the radio terminal, said first key having a validity period limited by a predefined expiration date;
 - ~~an-utilization step~~ by the identification module ~~of-utilization-of~~ at least one second key memorized in the identification module by at least one second authentication algorithm memorized in the identification module, said second key being identical or complementary to the first key and associated with the radio terminal, said second key having a validity period limited by said predefined expiration date; ~~and~~
 - ~~a-comparison-step-comparing~~ in the identification module ~~for-comparing~~ the results obtained by said first and second authentication algorithms.

8. (Currently Amended) The method according to claim 2, wherein ~~the said authenticating authentication step~~ comprises the utilization of said predefined expiration date.
9. (Currently Amended) The method according to claim 7, wherein said initialization ~~step~~ is initiated by a mobile radio-telephony network and also comprises:
generation by the identification module of at least one of said first and second keys;
a storage in the identification module of said second key; and
transmission to the radio terminal by the identification module of said first key, said first key being encrypted by use of the trust key.
10. (Currently Amended) The method according to of claim 7, wherein said comparing comparison step is done between, ~~on the one hand,~~ a response produced by said first authentication algorithm, stored in memory in the radio terminal and transmitted to said identification module and, ~~on the other hand,~~ a response result, stored in memory in the identification module, produced by said authentication algorithm.
11. (Original) The method according to claim 7, wherein said first key is an asymmetrical private key K_s and said second key being a public key K_p complementary to the first key.
12. (Original) The method according to claim 7, wherein said first key is symmetrical, said second key is stored in memory in the identification module being identical to the first key, these keys forming a single symmetrical authentication key.
13. (Currently Amended) The method according to claim 7, further comprising an updating step of said first and second keys, initiated by the identification module prior to said predefined expiration date, said updating step ~~including the following substeps~~:

authentication between the radio terminal and the identification module using said first and second keys;

generation by an updating algorithm of the identification module of at least one updated key taking into account ~~an~~ information for replacing at least one of said first and second keys;

memorization in the identification module of the updated key for replacing said second key; and

transmission to the radio terminal by the identification module of the updated key analogue of said first key.

14. (Currently Amended) The method according to claim 13, wherein said updating step further comprises ~~in addition the~~ control of at least one of one identifier of the radio terminal ~~and/or~~ of the identification module.

15. (Currently Amended) The method according to claim 13, wherein an encryption of the key is carried out for said transmission to the radio terminal of the updated key analogue of the first key, said key encryption being done by said trust key.

16. The method according to claim 13, wherein the updating step ~~also comprises the following steps:~~

generation by the identification module of a new trust key after said authentication between radio terminal and module;

memorization in the identification module of the new trust key;

transmission to the radio terminal by the identification module of the newly generated trust key.

17. (Currently Amended) The method according to claim 13, wherein said updating step is completed by a verification test comprising a return transmission on the part of the radio terminal of at least one datum representative of effective receipt of data transmitted by the identification module during the updating step.

18. (Currently Amended) The method according to claim 5, wherein said trust key is a symmetrical encryption/decryption key analogous ~~or identical~~ to said symmetrical authentication key.

- 19.(Original) The method according to claim 5, wherein said trust key is an erasable session key.
- 20.(Currently Amended) The method according to claim 7, wherein a so-called revocation step is carried out on the initiative of the identification module, of the radio terminal, or of the corresponding radio-telephony network, said revocation step comprising the erasure in a memory of said identification module of at least said first key associated with the radio terminal.
- 21.(Currently Amended) An identification module in a radio terminal for the implementation of the method according to claim 1, characterized in that it comprises means comprising a device for memorizing at least one authentication algorithm, a calculation device means for executing at least one step consisting of applying an said authentication key to said authentication algorithm as well as at least one authentication algorithm memorized in the identification module, a communication ~~device~~ means, means a device for initiating a revocation and a revocation device means for revoking said authentication key, means a device for memorizing a specific characteristic of the radio terminal and means a device for actuating an updating algorithm for updating said authentication key, the communication means device being capable of providing at least one authentication key to the radio terminal and receiving data send from a secured server of a mobile radio-telephony network.
- 22.(New) The method according to claim 5, wherein said trust key is a symmetrical encryption/decryption key identical to said symmetrical authentication key.

IV. REMARKS

The claims have been amended to better conform to U.S. practice.

Claims 1-21 are not unpatentable under 35 U.S.C. 102(b) as being anticipated by Julin.

Claim 1 is directed to a method for establishing and managing a trust module between an identification module and a radio terminal.

In particular, an object of the claimed invention is to provide and manage a trust model between a radio-communication terminal, such as a mobile phone, and an SIM card present in the terminal (see page 4, lines 7-9). Another object is to propose and define a process making it possible to secure the exchanges between the SIM card and the terminal, and wherein the operator of a mobile radio-telephony network replaces the certification authorities. This process makes it possible to create a secured and irrevocable relation between the SIM card and a terminal functionality authenticated by the network. This process also makes it possible for DRM-type technologies to store key pairs securely in the SIM (see page 4, lines 10-17).

For a more detailed explanation, the Examiner's attention is directed to pages 1-4 of the present specification. In particular:

Page 1, lines 5-7, "...establish a trust relation ship between a radio-communication terminal and a SIM chip card or the like, in order to secure exchanges between the card and the terminal."

Page 2, line 10, "Nevertheless, the aforementioned solution is not entirely secured" and lines 16-17 "...storage of the private keys Ks has been shown to be problematic,..."

Page 3, lines 25-30, "As a result, the rights to use a secured content are thus associated with a mobile terminal and not with an individual. In order to be able to associate the user rights with a user, it is necessary to better know the security means between the SIM card and the terminal insofar that the terminal is not protected against manipulators and insofar as it cannot be authenticated by the (U)SIM card or the other means difficult to subvert." (emphasis added).

Thus, the invention as recited in claim 1 relates to "A method for establishing and managing a trust model between an identification module and a radio terminal, said method comprising:

authenticating a radio terminal by said identification module, said authenticating being carried out by radio terminal authentication means that are provided either to said identification module by a mobile radio-telephony network at the time of an initialization or at the time of an updating, or to said radio terminal by the identification module; and

controlling by said identification module at least one specific characteristic of the radio terminal, said specific characteristic being previously transmitted by radio-telephony to said identification module from a secured server of said mobile radio-telephony network. (emphasis added).

It is respectfully submitted that Julin is irrelevant to the claimed invention.

Julin relates to and only discloses a method for personalization of an active card (see Title, Abstract, Technical Field, Technical Background, Object of the Invention, Summary of the Invention, Description of Embodiments, Claims) such as a SIM card.

Nowhere does Julin teach or disclose the technical features recited amended claim 1. This is not surprising because the objects and technical problems to be solved in Julin are fully different (see column 1, lines 36-41: "...to effect the personalization procedure in places other than the above-mentioned central place...") from ones disclosed in the

claimed invention. The purpose of Julin is totally different from that of the claimed invention.

Julin does not disclose retrieving by the SIM card any radio terminal specific characteristic (IMEI for example) via a secured server of a mobile radio-telephony network. In contrast, Julin recites that the SIM card is inserted in a reader 9 and receives personalization data such as keys (ki, PUK) IMSI. It is respectfully submitted that such data taught by Julin are not a specific characteristic of a radio terminal.

Thus, it is respectfully submitted that embodiments cited by the Examiner and disclosed by Julin in Figures 1-3 and column 3, line 20, to column 4, line 26, do not anticipate the claimed invention as explained above.

Julin simply does not disclose establishing a trust relationship between a radio-communication terminal and a SIM card, in order to secure exchanges between these two entities. In Julin, it is only a question of personalization of an active card (for example a SIM card).

It is noted that the teaching of Julin does not permit any authentication of the radio terminal by the SIM card. In complete contrast, Julin recites the terminal can send data into the SIM card (see column 3, lines 56, -column 4, line 4) and other data can be loaded via a reader 10 of a retailer's data terminal equipment 9 (column 4, lines 17-25).

Further there is no teaching about how to efficiently avoid use of another (non-authorized) terminal with a SIM card. It is not relevant for the purpose of distributing secure contents for mobile telephones (Specification, page 1, lines 13-14) via an identity module. In contrast, those skilled in the art find in Julin how to write data on an identity module.

10/719,303

Response to the Office Action mailed 22 February 2007

Applicants traverse the 35 U.S.C. 102(b) rejection because the "identical invention must be shown in as complete detail as is contained in the claim", MPEP 2131, quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226; 9 USPQ2d 1913, 1920 (Fed Cir. 1989). That is not a standard that can be met in a rejection under 35 USC 102 using *Julin*.

Claim 21 is directed to an authentication module and has limitations similar to claim 1.

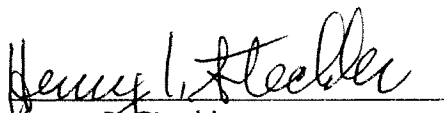
For all of the above reasons the rejection of claims 1-21 should be withdrawn.

Further, since there is no suggestion in *Julin* of the claimed features, the claims are unobvious over it (see MPEP 2143.01).

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment of \$50 for the added dependent claim as well as any other fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Henry I. Steckler

Reg. No. 24,139

Perman & Green, LLP

425 Post Road

Fairfield, CT 06824

(203) 259-1800

Customer No.: 2512

May 21, 2007

Date

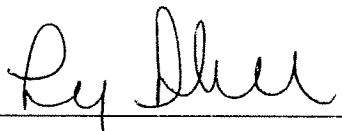
10/719,303

Response to the Office Action mailed 22 February 2007

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being transmitted electronically, on the date indicated below, addressed to the Mail Stop AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 22 May 2007

Signature: 
Lisa Shimizu
Person Making Deposit